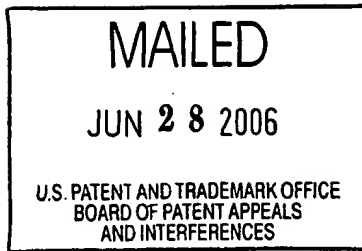The opinion in support of the decision being entered today
was **not** written for publication in and
is **not** binding precedent of the Board.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte HANS SJOBLOM

Appeal No. 2006-1011
Application No. 09/423,511

ON BRIEF

Before: CRAWFORD, NAPPI and FETTING Administrative **Patent Judges.**

NAPPI, **Administrative Patent Judge**.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134 of the final rejection of
claims 1 through 3, 6 through 29. Claims 4 and 5 were canceled in an
amendment submitted after the final rejection. For the reasons stated *infra* we
affirm in part the examiner's rejection of these claims.

Invention

The invention relates to a method of using a smart card to create a transaction message, which can be transferred to a receiver, which cannot be tampered with without such tampering being easily recognizable. See page 2 of appellant's specification.

Claim 1 is representative of the invention and reproduced below:

1. A method for performing electronic transactions via a communications network, in which a sender of transaction messages is assigned a smart card with an associated unique identity and a private key stored in the card in a protected manner and in which an associated public key is kept generally available, characterized in that in connection with an electronic transaction under the sender's own control, preferably through his own input of message information, the sender independently of any connection to a communications network and without computer dialog with a receiver, creates, on the basis of entered transaction information, a transaction message, which contains information necessary for the transaction, the transaction message being created in the smart card with the aid of software previously stored in the smart card, and in his smart card, provides the created transaction message with his digital signature while using his own private key for subsequent output and transmission of the transaction message.

Reference

The reference relied upon by the examiner is:

Heinonen et al. (Heinonen)	5,887,266	March 23, 1999 (filed Feb.7, 1996)
Barlow et al. (Barlow)	6,038,551	March 14, 2000 (filed March 11, 1996)

Rejection at Issue

Claims 1 through 3, 6 through 9, 11 through 13, 15 through 18, 21 through 23 and 25 through 29 stand rejected under 35 U.S.C. § 102(e) as being

unpatentable over Barlow. Claim 14 stands rejected under 35 U.S.C. § 103(a) as

being unpatentable over Barlow. Claims 10, 19, 20 and 24 stand rejected under

35 U.S.C. § 103(a) as being unpatentable over Barlow in view of Heinonen.

Throughout the opinion we make reference to the brief and the answer for the

respective details thereof.

Opinion

We have carefully considered the subject matter on appeal, the rejections

advanced by the examiner and the evidence of anticipation and obviousness

relied upon by the examiner as support for the rejections. We have, likewise,

reviewed and taken into consideration, in reaching our decision, appellant's

arguments set forth in the brief along with the examiner's rationale in support of

the rejections and arguments in rebuttal set forth in the examiner's answer.

With full consideration being given to the subject matter on appeal, the

examiner's rejections and the arguments of appellant and the examiner, and for

the reasons stated *infra* we do not sustain the examiner's rejection of claims 1

through 3, 6 through 9, 11 through 13, 15 through 18 and 27 through 29[1] under

35 U.S.C. § 102(e) nor do we sustain the examiner's rejection of claims 10, 14

and 19 under 35 U.S.C. § 103(a). However, we sustain the examiner's rejection

---

[1] We note that claims 6, 7 and 20 all contain a typographical error, in that they ultimately depend upon canceled claim 5 (claim 28 is also in error as it depends from claim 6). Appellant states in the amendment dated August 25, 2004 (received in the PTO September 4, 2004) that claims 4 and 5 are "deleted as being redundant, since their features are included in superior claims." Accordingly, we consider that appellant intended claims 6, 7 and 20 to be dependent upon claim 1. Appellant should make the appropriate corrections during any further prosecution of this application.

of claims 21, 22, 23, 25 and 26 under 35 U.S.C. § 102(e) and we sustain the

examiner's rejection of claim 24 under 35 U.S.C. § 103(a).

Appellant argues, on pages 3 through 6 of the brief, that claims 1 through

9, 11 through 13, 15 through 18, 21 through 23 and 25 through 29 are not

anticipated by Barlow. On page 3 of the brief, appellant asserts that Barlow

teaches a user- configurable smart card which can be used in various systems,

and that of the various systems that Barlow teaches that the smart card can be

used with, only three, ATM, Vending and Online shopping, can be characterized

as financial transaction systems. On page 4 of the brief, appellant argues that

Barlow's disclosed ATM transaction, requires a back and forth interaction

between the sender and receiver's computer and that this back and forth is

"contrary to the concept of the invention as defined in the pending main claim."

On pages 4 and 5 of the brief, appellant asserts that Barlow's discussion of using

the smart card to purchase from a vending machine, which the examiner relies

upon in making the rejection, teaches a smart card loaded with money and the

vending machine interacts with the smart card to electronically deduct payment

from the smart card. Appellant states:

> There are significant differences between this known technology and the
> method for performing electronic transactions as disclosed in Claim 1.
> The present invention creates a "transaction message" "in the smart card
> with the aid of software previously stored in the smart card". Also the
> created message is provided with the senders [sic, sender's] "digital
> signature while using his own private key for subsequent output and
> transmission of the transaction message." While it is true that the above
> described use according to *Barlow et al.* of a cash card in a vending
> machine completes a transaction off-line, no digitally signed transaction
> message is made and transmitted. Only an electronic deduction is made

in the chip on the card by a mechanism in the vending machine. No message is ever digitally signed and transmitted in the vending machine example.

Further, on page 5 of the brief, appellant asserts that the online shopping disclosure of Barlow also require a back and forth exchange of information.

Appellant thus concludes on page 6 of the brief:

> All of the examples of Barlow et al., involve interaction, before completion of the digitally signed message, with entities outside the sender's control, in particular in this case entities outside the actual smart card itself. Nowhere in Barlow et al. is there any indication of the concept of the present invention. All that Barlow et al reveals is the previously known interacting technology which opens the possibility of hacking, intrusions and errors during the compiling and digital signing of the transaction message. It is submitted that the independent claims 1, 21 and 23 are new and non-obvious over Barlow et al.

The examiner, in response, asserts that the limitations directed to the sender sending a message independent of any connection to a communications network and without dialog with a receiver are optional as the claim recites "preferably." Further, the examiner asserts that Barlow's teaching of using the smart card with a vending machine meets the limitation of sending transaction messages that are independent of a connection with a network and without dialog with a receiver. See answer, page 9.

In the reply brief, appellant asserts that the examiner's claim interpretation is in error and that the reasonable interpretation of the claim 1 term "preferably" is that it is only directed to the limitation "through his own input of message information."

5

We agree with the appellant regarding the use of the term "preferably" in claim 1, and consider it to only operate on the further statement "through his own input of message information." Thus, contrary to the examiner's assertions, we do not find that the further limitations of "the sender independently of any connection to a communications network and without computer dialog with a receiver, creates ... a transaction message... for subsequent output and transmission of the transaction message" are optional. We find that claim 1 recites limitations directed to the transaction message containing information necessary for the transaction and that the transaction message is generated on the smart card. Further, claim 1 recites limitations directed to the message being created independently of a connection with a network and without dialog with a receiver the transaction message is created.

While we do find that Barlow teaches creation of a transaction message on the smart card using private keys and is the creation is independent of a communications network, we do not find that Barlow teaches that the transaction message is generated without dialog with a receiver. Barlow teaches that the smart card contains public and private keys and that these keys are used to encrypt messages and digitally sign messages. See figure 3, item 68 and column 12, lines 15 through 22. Barlow teaches that the keys do not leave the card and that the card can perform the encryption and signing of the messages. See column 12, lines 26 and lines 40 through 45. Barlow teaches that the smart card can store tokens for beverage/snack vending machines and public

transportation and can be used for ATM banking and online shopping. See

column 14, lines 10, 11, 44 and 60. While these tokens, stored on the smart

card, are transaction messages, in that they provide authorization to perform a

transaction, there is no disclosure in Barlow that they are provided with a digital

signature using the public key. Nor do we find that a digital signature is inherent

to the tokens stored in the smart card. In the example of the ATM banking the

transaction message, the "signed request for cash" is transferred from the card to

the ATM, the receiver. The ATM then debits the user's account. See column 14,

lines 52 through 57. Thus, though the ATM is disclosed as being connected to a

bank network which is a communications network and the generation of the

transaction message "the request for cash" is not dependent upon the

communications network, nonetheless there is dialog with the receiver, the ATM.

Further, in the example of on-line shopping Barlow identifies that there is an

exchange of information between the merchant and the user's computer

(containing the smart card) to generate the transaction message. See column 16

lines 21 through 43. Thus, we find no teaching in Barlow of creating a

transaction message without dialog with a receiver as recited in claim 1.

Accordingly we will not sustain the examiner's rejection of claim 1 or the claims

dependent thereupon. Claims 2 through 3, 6 through 9, 11 through 13, 15

through 18 and 27 through 29.

The examiner has not asserted, nor do we find that Heinonen teaches or

suggests modifying Barlow to correct the noted deficiencies in the rejection of

claim 1. Accordingly, we will not sustain the examiner's rejection of claims 10, 19 and 20.

We next consider independent claims 21, 23, 26 and the claims dependent thereupon. Appellant has presented no arguments directed to the limitations of independent claims 21, 23 and 26, rather appellant grouped these claims with claim 1. However, we do not find that claims 21, 23 and 26 are commensurate in scope with appellant's arguments. Specifically, claims 21, 23 and 26 do not contain limitations directed to creating a transaction message without dialog with a receiver.

Independent claims 21 and 23 recite limitations directed to a smart card, which protects a private key, contains an asymmetrical algorithm, receives input to create a message, and contains a processor to create a transaction message with a digital signature. Appellant has not argued that Barlow does not teach these features. Further, as discussed above with respect to claim 1, we find that Barlow teaches that the smart card contains keys and using the keys can digitally sign a message. Further, Barlow teaches that the encryption uses asymmetrical algorithms. See column 11, lines 56 through 60. Thus, appellant has not convinced us of error in the examiner's rejection of claims 21 and 23. We accordingly sustain the examiner's rejection of claims 21, 23 and the claims dependent thereupon, claims 24 and 25.

Independent claim 26 is neither grouped nor addressed in appellant's arguments and is broader in scope than the limitations of claim 1 argued by the appellant. Claim 26 recites:

> Use of a smart card with a private key stored therein for providing independently of the communications network, an electronic transaction message provided with a digital signature based upon the private key.

As appellant has presented no argument directed to why the limitations of claim 26 are patentable over the art cited by the examiner in rejecting claim 26 we are not persuaded of error in the examiner's rejection. Further, as discussed *supra* with respect to claim 1, we find that Barlow teaches generation of a transaction message with a digital signature independent of a communication network. Accordingly we sustain the examiner's rejection of claim 26.
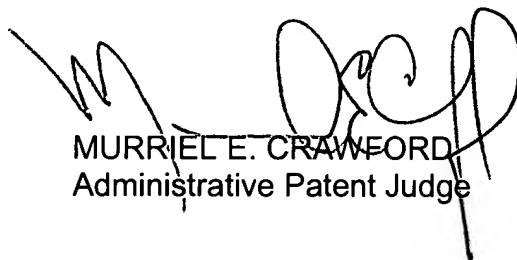
In summary, we do not sustain the examiner's rejection of claims 1

through 3, 6 through 9, 11 through 13, 15 through 18 and 27 through 29 under 35

U.S.C. § 102(e) nor do we sustain the examiner's rejection of claims 10, 14 and

19 under 35 U.S.C. § 103(a). However, we sustain the examiner's rejection of

claims 21, 22, 23, 25 and 26 under 35 U.S.C. § 102(e) and we sustain the

examiner's rejection of claim 24 under 35 U.S.C. § 103(a). The decision of the

examiner is affirmed in part.

No time period for taking any subsequent action in connection with this

appeal may be extended under 37 CFR § 1.136(a)(1)(iv).

AFFIRMED-IN-PART

MURRIEL E. CRAWFORD   )
Administrative Patent Judge   )
)
)
) BOARD OF PATENT
ROBERT E. NAPPI   )   APPEALS AND
Administrative Patent Judge   )   INTERFERENCES
)
)
)
ANTON W. FETTING   )
Administrative Patent Judge   )

REN/lg

10

Appeal No. 2006-1011
Application No. 09/423,511

Albihns Stockholm AB
Box 5581, Linnegatan 2
SE-114 85 Stockholm; Sweden
Stockholm SE Sweden